IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A method for providing network security features, comprising the steps of:

(a) identifying a plurality of network objects;

(b) retrieving rule sets associated with at least one of the identified network objects, the rule sets including a plurality of policy rules that govern actions relating to the identified network objects;

(c) reconciling overlapping policy rules of the rule sets amongst the network objects; and

(d) executing the reconciled rule sets;

wherein the rule sets are combined into a single rule set, and duplicate policy rules of the rule sets are removed;

wherein a user is notified of conflicting policy rules of the rule sets.

a1

2. (Original) The method as recited in claim 1, wherein each policy rule of the reconciled rule sets includes a rule action selected from the group consisting of: permitting an action relating to the identified network objects, denying an action relating to the identified network objects, and conditionally denying an action relating to the identified network objects.

3. (Original) The method as recited in claim 2, wherein an action relating to the identified network objects is permitted if no policy rules deny the action, at least one policy rule conditionally denies the action, and at least one policy rule permits the action.

4. (Original) The method as recited in claim 2, wherein the policy rules denying the action are evaluated first, the policy rules conditionally denying the action are evaluated second, and the policy rules permitting the action are evaluated third.

5. (Original) The method as recited in claim 1, wherein an action relating to the identified network objects is denied if none of the policy rules permit the action.

6. (Original) The method as recited in claim 1, wherein an action relating to the identified network objects is denied if none of the policy rules match a request for the action.

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Original) The method as recited in claim 1, wherein the rule sets are associated with a particular network object.

11. (Original) The method as recited in claim 1, wherein a protocol configuration enforced by a related proxy is selected from a hierarchal list if an action is permitted by more than one rule.

12. (Currently Amended) A computer program product for providing network security features, comprising:

(a) computer code for identifying a plurality of network objects;

(b) computer code for retrieving rule sets associated with at least one of the identified network objects, thc rule sets including a plurality of policy rules that govern actions relating to the identified network objects;

(c) computer code for reconciling overlapping policy rules of the rule sets amongst the network objects; and

(d) computer code for executing the reconciled rule sets;

wherein the rule sets are combined into a single rule set, and duplicate policy rules of the rule sets are removed;

wherein a user is notified of conflicting policy rules of the rule sets.

13. (Original) The computer program product as recited in claim 12, wherein each policy rule of the reconciled rule sets includes a rule action selected from the group consisting of: permitting an action relating to the identified network objects, denying an action relating to the identified network objects, and conditionally denying an action relating to the identified network objects.

14. (Original) The computer program product as recited in claim 13, wherein an action relating to the identified network objects is permitted if no policy rules deny the action, at least one policy rule conditionally denies the action, and at least one policy rule permits the action.

15. (Original) The computer program product as recited in claim 13, wherein the policy rules denying the action are evaluated first, the policy rules conditionally denying the action are evaluated second, and the policy rules permitting the action are evaluated third.

16. (Original) The computer program product as recited in claim 12, wherein an action relating to the identified network objects is denied if none of the policy rules permit the action.

17. (Original) The computer program product as recited in claim 12, wherein an action relating to the identified network objects is denied if none of the policy rules match a request for the action.

18. (Cancelled)

19. (Cancelled)

20. (Cancelled)

21. (Original) The computer program product as recited in claim 12, wherein the rule sets are associated with a particular network object.

22. (Original) The computer program product as recited in claim 12, wherein a protocol configuration enforced by a related proxy is selected from a hierarchal list if an action is permitted by more than one rule.

23. (Currently Amended) A rule based network security system for providing network security features, comprising:

(a) logic for identifying a plurality of network objects;

(b) logic for retrieving rule sets associated with at least one of the identified network objects, the rule sets including a plurality of policy rules that govern actions relating to the identified network objects;

(c) logic for reconciling overlapping policy rules of the rule sets amongst the network objects; and

(d) logic for executing the reconciled rule sets;

wherein the rule sets are combined into a single rule set, and duplicate policy rules of the rule sets are removed;

wherein a user is notified of conflicting policy rules of the rule sets.

24. (Currently Amended) A method for establishing network security, comprising the steps of:

(a) providing a plurality of network objects of a network and a plurality of rule sets; and

(b) associating the network objects with the rule sets;

(c) wherein the rule sets include a plurality of policy rules that govern actions relating to the identified network objects during operation of the network;

wherein a plurality of the rule sets are combined into a single rule set, and duplicate policy rules of the rule sets are removed;

wherein a user is notified of conflicting policy rules of the rule sets.

25. (Original) The method as recited in claim 24, wherein a user is allowed to associate the network objects with the rule sets via a graphical user interface.

26. (Original) The method as recited in claim 24, wherein each policy rule of the reconciled rule sets includes a rule action selected from the group consisting of: permitting an action relating to the identified network objects, denying an action relating to the identified network objects, and conditionally denying an action relating to the identified network objects.

27. (Original) The method as recited in claim 26, wherein an action relating to the identified network objects is permitted if no policy rules deny the action, at least one policy rule conditionally denies the action, and at least one policy rule permits the action.

28. (Original) The method as recited in claim 24, wherein an action relating to the identified network objects is denied if none of the policy rules permit the action.

29. (Currently Amended) A computer program product for establishing network security, comprising:

(a) computer code for providing a plurality of network objects of a network and a plurality of rule sets; and

(b) computer code for associating the network objects with the rule sets;

(c) wherein the rule sets include a plurality of policy rules that govern actions relating to the identified network objects during operation of the network; wherein a plurality of the rule sets are combined into a single rule set, and duplicate policy rules of the rule sets are removed;

wherein a user is notified of conflicting policy rules of the rule sets.

30. (Original) The computer program product as recited in claim 29, wherein a user is allowed to associate the network objects with the rule sets via a graphical user interface.

31. (Original) The computer program product as recited in claim 29, wherein each policy rule of the reconciled rule sets includes a rule action selected

from the group consisting of: permitting an action relating to the identified network objects, denying an action relating to the identified network objects, and conditionally denying an action relating to the identified network objects.

32. (Original) The computer program product as recited in claim 31, wherein an action relating to the identified network objects is permitted if no policy rules deny the action, at least one policy rule conditionally denies the action, and at least one policy rule permits the action.

33. (Original) The computer program product as recited in claim 29, wherein an action relating to the identified network objects is denied if none of the policy rules permit the action.

a1

34. (New) The method as recited in claim 1, wherein a graphical user interface is provided for providing an option to a user to apply both an AND operation and an OR operation to selected network objects.

35. (New) The method as recited in claim 1, wherein included is a first graphical user interface that allows a user to associate the network objects with the rule sets, a second graphical user interface that allows the user to create associations of the rule sets and the network objects for a firewall, a third graphical user interface that is displayed upon selection of a network object, a fourth graphical user interface for creating and editing the rule sets, a fifth graphical user interface for configuring a new policy rule for being added to one of the rule sets, a sixth graphical user interface for adding a new network object, and a seventh graphical user interface for editing one of the network objects.